UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF NORTH CAROLINA

ANTHONY REID and MADISON LUCAS, individually and on behalf of those similarly situated, Plaintiffs, vs. **AHOLD DELHAIZE USA SERVICES, LLC,** Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Anthony Reid and Madison Lucas ("Plaintiffs"), individually and on behalf of all others similarly situated, brings this action against Defendant Ahold Delhaize USA Services, LLC ("Ahold" or "Defendant") to obtain damages, restitution, and injunctive relief from Defendant. Plaintiffs make the following allegations upon information and belief, except as to their own actions, the investigation of their counsel, and facts that are a matter of public record.

NATURE OF THE ACTION

1. This class action arises out of Defendant Ahold's failures to properly secure, safeguard, encrypt, and/or timely and adequately destroy Plaintiffs' and Class Members' (defined below) sensitive personal identifiable information that it had acquired and stored for its business purposes.

2. Defendant represents itself as the "largest grocery retail group on the East

Coast."[1] Its brands include Food Lion, Giant, The Giant Company, Hannaford, and Stop & Shop.[2]

3. As part of its employment and benefits packages, Ahold provides Health Insurance benefits along with Group Life Insurance, Short and Long Term Disability and 401 (k) Savings Plans[3] to individual employees and their families," including Plaintiffs and Class members.

4. According to a Data Breach Notification provided to the Maine Attorney General's Office, Defendant announced that it had experienced a hacking incident.[4] Defendant's "Notice of Data Breach" states that a data breach occurred on its network between November 5, 2024 and November 6, 2024 (the "Data Breach").[5] The Data Breach affected over 2.2 million individuals.[6]

5. According to cybernews sources, a ransomware group accessed Defendant's information network and exfiltrated data from Defendant's network.[7] On June 30, 2025, Inc Ransom reported having stolen 6 Tb of information from Ahold's information network.[8]

6. Due to Defendant's data security failures which resulted in the Data Breach, cybercriminals were able to target Defendant's computer systems and exfiltrate highly

[1] https://www.adusa.com/about-us (last visited July 7, 2025).
[2] *Id.*
[3] www.adusa.com/025_Benefits_at_a_Glance.pdf (last visited July 7, 2025).
[4] https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/b17963fc-3806-430e-b28e-bac47eb73a8b.html (last visited July 7, 2025).
[5] *Id. See* "Notice of Data Breach."
[6] *Id.*
[7] https://www.securityweek.com/ahold-delhaize-data-breach-impacts-2-2-million-people/ (last visited July 7, 2025).
[8] *Id.*

sensitive and personally identifiable information ("PII") and protected health information ("PHI") (collectively, the "Private Information") belonging to Plaintiffs and Class members. As a result of this Data Breach, Plaintiffs' and Class members' Private Information of remains in the hands of those cybercriminals.

7. Defendant's notice to the Maine AG states that it "detected a cybersecurity issue involving unauthorized access to some of our internal U.S. business systems on November 6, 2024,"[9] "may have included internal employment records containing personal information about you that we obtained in the course of providing services for certain current and former Ahold Delhaize USA companies."[10]

8. Further, that it:

> immediately launched an investigation with the assistance of leading external cybersecurity experts, coordinated with U.S. federal law enforcement and began taking steps to contain the issue. Based on our investigation, we identified that an unauthorized third party obtained certain files from one of our internal U.S. file repositories between November 5 and 6, 2024.[11]

9. However, despite apparently learning of the Data Breach on or about November 6, 2024, and determining that Private Information was involved in the breach, Defendant did not begin sending notices to the victims of the Data Breach (the "Notice of Data Breach Letters") until June 26, 2025.

10. The Private Information compromised in the Data Breach included current and former employees' PII and PHI, including Plaintiffs. This Private Information included, but is not limited to: name, contact information (for example, postal and email

[9] *Id.* n.4 , *supra*.
[10] *Id.*
[11] *Id.*

address and telephone number), date of birth, government-issued identification numbers (for example, Social Security, passport and driver's license numbers), financial account information (for example, bank account number), health information (for example, workers' compensation information and medical information contained in employment records), and employment-related information.[12]

11. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect Plaintiffs' and Class members' Private Information with which it was entrusted for either employment or treatment or both.

12. Plaintiffs brings this class action lawsuit on behalf of themselves and all other similarly situated persons to address Defendant's inadequate safeguarding of Class members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiffs and other Class members that their information had been subject to the unauthorized access of an unknown third party and failing to include in that belated and inadequate notice precisely what specific types of information were accessed and taken by cybercriminals.

13. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiffs' and Class Members'

[12] *Id.* n.4, *supra*.

Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that network in a dangerous condition.

14. Defendant disregarded the rights of Plaintiffs and Class Members by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Plaintiffs' and Class Members' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiffs and Class Members with prompt and full notice of the Data Breach.

15. In addition, Defendant failed to properly monitor the computer network and systems that housed the Private Information. Had Defendant properly monitored its computer network and systems, it would have discovered the massive intrusion sooner rather than allowing cybercriminals almost a month of unimpeded access to Plaintiffs' and Class members' PII and PHI.

16. Plaintiffs' and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained is now in the hands of data thieves.

17. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including: opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class

Members' information, filing false medical claims using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

18. As a result of the Data Breach, Plaintiffs and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiffs and Class Members must now and for years into the future closely monitor their financial accounts to guard against identity theft.

19. Plaintiffs and Class Members may also incur out-of-pocket costs for, *e.g.*, purchasing credit monitoring, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

20. Through this Complaint, Plaintiffs seeks to remedy these harms on behalf of themselves and all other similarly situated individuals whose Private Information was accessed during the Data Breach.

21. Accordingly, Plaintiffs brings this action against Defendant seeking redress for its unlawful conduct, and asserting claims for: (i) negligence and negligence *per se*; (ii) breach of implied contract, (iii) breach of fiduciary duty; (iv) unjust enrichment; and (v) declaratory and injunctive relief.

22. Plaintiffs seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, as well as long-term and adequate credit monitoring funded by Defendant, and declaratory relief.

PARTIES

23. Plaintiff Anthony Reid is and at all times mentioned herein was an individual citizen of Maryland. Plaintiff Reid was an Ahold employee and enrolled in its benefits programs. Plaintiff Reid received notice of the Data Breach dated June 26, 2025, attached as Exhibit A.

24. Plaintiff Madison Lucas is and at all times mentioned herein was an individual citizen of Pennsylvania. Plaintiff Lucas was an Ahold employee and enrolled in its benefits programs. Plaintiff Lucas received notice of the Data Breach dated June 26, 2025, attached as Exhibit B.

25. Like Plaintiffs, other potential Class members received similar notices informing them that their Private Information was exposed in the Data Breach on or about June 26, 2025.

26. Defendant Ahold Delhaize USA Services, LLC is a Delaware limited liability company with its principal place of business located at 2110 Executive Dr, Salisbury, North Carolina, 28147.

27. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged here are currently unknown to Plaintiffs.

28. Plaintiffs will seek leave of court to amend this Complaint to reflect the true names and capacities of the responsible parties when their identities become known.

JURISDICTION AND VENUE

29. This Court has subject matter jurisdiction over this matter pursuant to 28 U.S.C. § 1332(d). The amount in controversy in this Class action exceeds $5,000,000,

exclusive of interest and costs, and there are numerous Class members who are citizens of states other than Defendant's state of citizenship.

30. This Court has personal jurisdiction over the parties in this case. Defendant Ahold conducts business in this District and is a citizen of this District by virtue of having its principal place of business located in this District.

31. Venue is proper in this District under 28 U.S.C. §1391(b) because Ahold maintains a headquarters in this District and regularly conducts business in this District.

FACTUAL ALLEGATIONS

Defendant's Business

32. Defendant Ahold represents itself as "the largest grocery retail group on the East Coast and the fourth largest in the nation, serving millions of omnichannel customers each week.[13]

33. In the ordinary course of its business, Defendant requires each employee to provide (and Plaintiffs did provide) Defendant with sensitive, personal, and private information, such as their:

- Name, address, phone number, and email address;
- Date of birth;
- Social Security number;
- Marital status;
- contact information;
- Primary and secondary insurance policy holders' name, and address;

[13] https://www.adusa.com/ (last visited July 7, 2025).

- Demographic information;
- Driver's license or state or federal identification;
- Information relating to the individual's medical and medical history;
- Insurance information and coverage; and
- Banking and/or credit card information.

34. Defendant also creates and stores medical records and other protected health information for its employees, including records of treatments and diagnoses.

35. Defendant agreed to and undertook legal duties to maintain the protected health and personal information entrusted to it by Plaintiffs and Class members safely, confidentially, and in compliance with all applicable laws, including the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, and the Health Insurance Portability and Accountability Act ("HIPAA").

36. Yet, through its failure to properly secure Plaintiffs' and Class members' Private Information, Defendant failed to meet its own promises of employee privacy.

37. The employee information held by Defendant in its computer system and network included Plaintiffs' and Class members' highly sensitive Private Information.

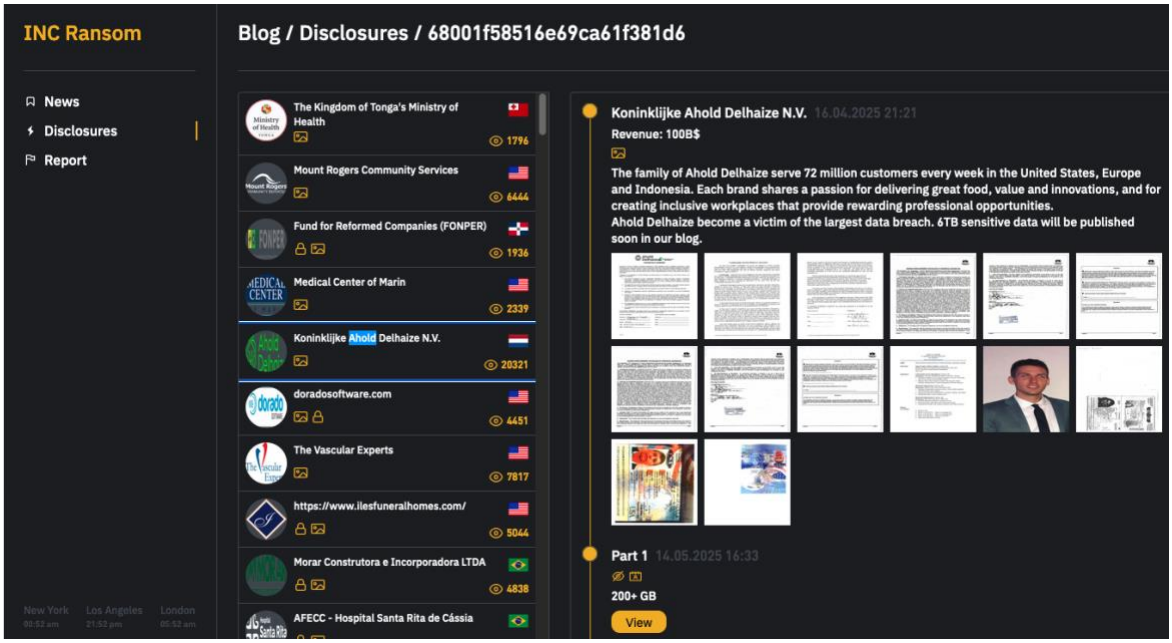
The Data Breach

38. A data breach occurs when cyber criminals intend to access and steal Private Information that has not been adequately secured by a business entity like Defendant.

39. According to Defendant's Notice, it learned of a cyberattack on its computer systems on or about April 17, 2025, when it detected suspicious activity in its information

network.[14]

40. As above, during April 2025, a well-known ransomware group, "Inc Ransom" claimed to have exfiltrated 6 Tb of employee data and reported publishing a "sample" of over 800 Gb on its dark web site.[15]



41. Presently, however, Defendant has provided no public information on the ransom demand or payment.

42. In January 2023, two years before the attack, HHS created a presentation specifically for healthcare providers and IT departments, warning entities like Defendant of the severe threats posed by cybercriminal groups.[16] Within the healthcare industry, the risk of a cyberattack is well-known and preventable with adequate security systems in

[14] https://www.securityweek.com/ahold-delhaize-confirms-data-stolen-in-ransomware-attack/ (last visited July 7, 2025).
[15] Image at https://www.securityweek.com/ahold-delhaize-data-breach-impacts-2-2-million-people/ (last visited July 7, 2025).
[16] https://www.hhs.gov/sites/default/files/royal-blackcat-ransomware-tlpclear.pdf (last visited July 7, 2025).

place.

43. On or about June 26, 2025, months after Defendant learned that the Class members' Private Information was attacked by cybercriminals, Defendant's employees began receiving their notices of the Data Breach informing them that its investigation determined that their Private Information was accessed.

44. Defendant's notice letters list time-consuming, generic steps that victims of data security incidents can take, such as getting a copy of a credit report or notifying law enforcement about suspicious financial account activity. Defendant offered two years of credit monitoring for members of the class and Defendant offered no other substantive steps to help victims like Plaintiffs and Class members to protect themselves. On information and belief, Defendant sent a similar generic letter to all other individuals affected by the Data Breach.

45. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

46. Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

47. Defendant had obligations created by HIPAA, FTCA, contract, industry standards, common law, and representations made to Plaintiffs and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

48. Plaintiffs and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would

comply with its obligations to keep such information confidential and secure from unauthorized access.

The Data Breach was a Foreseeable Risk of which Defendant was on Notice.

49. It is well known that PII and PHI, including Social Security numbers in particular, is a valuable commodity and a frequent, intentional target of cyber criminals. Companies that collect such information, including Defendant, are well-aware of the risk of being targeted by cybercriminals.

50. Individuals place a high value on the privacy of their PII and PHI. Identity theft causes severe negative consequences to its victims, as well as severe distress and hours of lost time trying to fight against the impact of identity theft.

51. A data breach increases the risk of becoming a victim of identity theft. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice, "[a] direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, , or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket

loss."[17]

52. Individuals, like Plaintiffs and Class Members, are particularly concerned with protecting the privacy of their Social Security numbers, which are the key to stealing any person's identity and is likened to accessing one's DNA for hacker's purposes.

53. Data Breach victims suffer long-term consequences when their Social Security numbers are taken and used by hackers. Even if they know their Social Security numbers are being misused, Plaintiffs and Class Members cannot obtain new numbers unless they become a victim of Social Security number misuse.

54. The Social Security Administration has warned that "a new number probably won't solve all your problems. This is because other government agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So, using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same."[18]

55. Additionally in 2021, there was a 15.1% increase in cyberattacks and data breaches from 2020. Over the next two years, in a poll of security executives, they have predicted an increase in attacks from "social engineering and ransomware" as nation-states and cybercriminals grow more sophisticated. Unfortunately, these preventable cases will

[17] "Victims of Identity Theft, 2018," U.S. Department of Justice (April 2021, NCJ 256085) available at: https://bjs.ojp.gov/content/pub/pdf/vit18.pdf (last visited July 7, 2025).
[18] https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited July 7, 2025).

largely come from "misconfigurations, human error, poor maintenance, and unknown assets."[19]

56. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, and hopefully can ward off a cyberattack.

57. According to an FBI publication, "[r]ansomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return. Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data."[20] This publication also explains that "[t]he FBI does not support paying a ransom in response to a ransomware attack. Paying a ransom doesn't guarantee you or your organization will get any data back. It also encourages perpetrators to target more victims and offers an incentive for others to get involved in this type of illegal activity."[21]

58. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite its own acknowledgment of its duties to keep PII and PHI private and secure, Defendant failed to take appropriate steps to protect the PII and PHI of Plaintiffs and the proposed Class from being compromised.

---

[19] https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=176bb6887864 (last visited July 7, 2025).
[20] https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware (last visited July 7, 2025).
[21] *Id.*

Defendant Failed to Comply with FTC Guidelines.

59. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

60. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[22] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[23]

61. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have

[22] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited July 7, 2025).
[23] *Id*.

implemented reasonable security measures.

62. The FTC has brought enforcement actions against businesses, like that of Defendant, for failing to adequately and reasonably protect employee data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

63. These FTC enforcement actions include actions against healthcare providers like Defendant. *See, e.g., In the Matter of LabMD, LLC, A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

64. Defendant failed to properly implement basic data security practices.

65. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to employees' PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

66. Defendant was at all times fully aware of its obligation to protect the PII and PHI of its employees. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Failed to Comply with Industry Standards.

67. As shown above, experts studying cyber security routinely identify

healthcare providers as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

68. Several best practices have been identified that a minimum should be implemented by healthcare providers like Defendant, including but not limited to: educating all employees; utilizing strong passwords; creating multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; using multi-factor authentication; protecting backup data, and; limiting which employees can access sensitive data.

69. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

70. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

71. These frameworks are existing and applicable industry standards in the healthcare industry, yet Defendant failed to comply with these accepted standards, thereby

opening the door to and failing to thwart the Data Breach.

Data Breaches Put Consumers at an Increased Risk Of Fraud and Identify Theft

72. Data Breaches such as the one Plaintiffs and Class Members experienced cause significant disruption to the overall daily lives of victims affected by the attack.

73. In 2019, the United States Government Accountability Office released a report addressing the steps consumers can take after a data breach.[24] Its appendix of steps consumers should consider, in extremely simplified terms, continues for five pages. In addition to explaining specific options and how they can help, one column of the chart explains the limitations of the consumers' options. *See* GAO chart of consumer recommendations, reproduced and attached as Exhibit B. It is clear from the GAO's recommendations that the steps Data Breach victims (like Plaintiffs and Class) must take after a breach like Defendant's are both time consuming and of only limited and short-term effectiveness.

74. The GAO has long recognized that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."

75. The FTC, like the GAO, recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit

[24] https://www.gao.gov/assets/gao-19-230.pdf (last visited July 7, 2025).

freeze on their credit, and correcting their credit reports.[25]

76. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

77. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information.

78. Theft of Private Information is also gravely serious. PII/PHI is valuable property.[26]

79. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used. According to GAO:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See 2007 GAO Report, at p. 29.

80. Private Information and financial information are such valuable commodities

[25] *See* https://www.identitytheft.gov/Steps (last visited July 7, 2025).
[26] *See, e.g.,* John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

81. There is a strong probability that the entirety of the stolen information has been dumped on the black market or will be dumped on the black market, meaning Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future. This is evidenced by the fraud that has already taken place in Plaintiffs' case, as discussed in further detail below. Thus, Plaintiffs and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

82. As the HHS warns, "PHI can be exceptionally valuable when stolen and sold on a black market, as it often is. PHI, once acquired by an unauthorized individual, can be exploited via extortion, fraud, identity theft and data laundering. At least one study has identified the value of a PHI record at $1000 each."[27]

83. Furthermore, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[28] Such fraud may go undetected until debt collection calls commence months, or even years later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[29] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement

[27] https://www.hhs.gov/sites/default/files/cost-analysis-of-healthcare-sector-data-breaches.pdf at 2 (citations omitted) (last visited July 7, 2025).
[28] *Identity Theft and Your Social Security Number*, Social Security Administration (last visited July 7, 2025). (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited July 7, 2025).
[29] *Id.* at 4.

notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

84. Moreover, it is not an easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[30]

85. This data, as one would expect, commands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[31]

PLAINTIFFS' EXPERIENCES

Plaintiff Anthony Reid

86. Plaintiff Anthony Reid was an Ahold employee and participated in Defendant's benefit programs.

87. Plaintiff Reid received a Notice of Data Breach Letter, related to Defendant's

[30] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited July 7, 2025).

[31] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited July 7, 2025).

Data Breach that is dated June 26, 2025. *See* Exhibit A.

88. The Notice Letter that Plaintiff received does not explain exactly which parts of his PII and PHI were accessed and taken but instead generically states that the files contained his name, "internal employment records." *Id*.

89. Plaintiff Reid is especially alarmed by the vagueness in the Notice Letter regarding his stolen extremely private medical information, including his PII/PHI, as among the breached data on Defendant's computer system.

90. Since the Data Breach, Plaintiff Reid has tried to mitigate the damage by changing his passwords, contacting the credit bureaus as Defendant instructed, and monitoring his financial accounts for about 2 and a half hours per week. This is more time than he spent prior to learning of the Defendant's Data Breach. Having to do this every week as a result of Defendant's negligence not only wastes his time, but it also causes him great anxiety.

91. Soon after the Data Breach, Plaintiff Reid began receiving an excessive number of spam calls on the same cell phone number provided to Defendant on his records. These calls are a distraction, must be deleted, and waste time each day. Given the timing of the Data Breach, he believes that the calls are related to his stolen Private Information.

92. Plaintiff Reid is aware that cybercriminals often sell Private Information, and once stolen, it is likely to be abused months or even years after Defendant's Data Breach.

93. Plaintiff Reid has suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of unauthorized third parties and possibly criminals.

Plaintiff Reid suffered lost time, annoyance, interference, and inconvenience because of the Data Breach.

94. Plaintiff Reid has experienced anxiety and increased concerns arising from the fact that his Private Information has been or will be misused and from the loss of his privacy.

95. The risk is not hypothetical. Here, a known hacking group intentionally infiltrated the data, misused it, threatened to publish, or has published it on the Dark Web, and the sensitive information, including names and Social Security numbers, is the type that could be used to perpetrate identity theft or fraud.

96. Plaintiff further suffered actual injury in the form of damage to and diminution in the value of Plaintiff's Private Information —a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and because of the Data Breach. Future identity theft monitoring is reasonable and necessary, and such will include future costs and expenses.

97. Plaintiff has a continuing interest in ensuring that his Private Information which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

98. Had Plaintiff Reid been aware that Defendant's computer systems were not secure, he would not have entrusted Defendant with his PII and PHI.

Plaintiff Madison Lucas

99. Plaintiff Lucas was an Ahold employee during the period between 2013 and 2015. Plaintiffs Lucas received a Notice of Data Breach Letter, related to Defendant's Data

Breach that is dated June 26, 2025. *See* Exhibit B.

100. The Notice Letter that Plaintiff received does not explain exactly which parts of her PII and PHI were accessed and taken but instead generically states that the files contained her name and "internal employment records." *Id*.

101. Plaintiff Lucas is especially alarmed by the vagueness in the Notice Letter regarding her stolen extremely private medical information, including her PII/PHI, as among the breached data on Defendant's computer system.

102. Since the Data Breach, Plaintiff Lucas has tried to mitigate the damage by changing her passwords, contacting the credit bureaus as Defendant instructed, and monitoring her financial accounts for about 2 and a half hours per week. This is more time than she spent prior to learning of the Defendant's Data Breach. Having to do this every week not only wastes her time as a result of Defendant's negligence, but it also causes him great anxiety.

103. Soon after the Data Breach, Plaintiff Lucas began receiving an excessive number of spam calls on the same cell phone number provided to Defendant on her records. These calls are a distraction, must be deleted, and waste time each day. Given the timing of the Data Breach, she believes that the calls are related to her stolen Private Information.

104. Plaintiff Lucas is aware that cybercriminals often sell Private Information, and once stolen, it is likely to be abused months or even years after Defendant's Data Breach.

105. Plaintiff Lucas has suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse resulting from her Private

Information being placed in the hands of unauthorized third parties and possibly criminals. Plaintiff Lucas suffered lost time, annoyance, interference, and inconvenience because of the Data Breach.

106. Plaintiff Lucas has experienced anxiety and increased concerns arising from the fact that her Private Information has been or will be misused and from the loss of her privacy.

107. The risk is not hypothetical. Here, a known hacking group intentionally stole the data, misused it, threatened to publish, or has published it on the Dark Web, and the sensitive information, including names and Social Security numbers, is the type that could be used to perpetrate identity theft or fraud.

108. Plaintiff Lucas further suffered actual injury in the form of damages to and diminution in the value of Plaintiff's Private Information —a form of intangible property that Plaintiff Lucas entrusted to Defendant, which was compromised in and because of the Data Breach. Future identity theft monitoring is reasonable and necessary, and such will include future costs and expenses.

109. Plaintiff Lucas has a continuing interest in ensuring that her Private Information which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

110. Had Plaintiff Lucas been aware that Defendant's computer systems were not secure, she would not have entrusted Defendant with her PII and PHI.

PLAINTIFFS' AND CLASS MEMBERS' COMMON INJURIES

111. To date, Defendant has done absolutely nothing to compensate Plaintiffs and

Class Members for the damage they sustained in the Data Breach.

112. Defendant offered only two years of credit monitoring to class members.

113. Defendant fails to offer any compensation to victims of the Data Breach, who commonly face multiple years of ongoing identity theft, and it entirely fails to provide any compensation for its unauthorized release and disclosure of Plaintiffs' and Class Members' Private Information, out of pocket costs, and the time they are required to spend attempting to mitigate their injuries.

114. Furthermore, Defendant's failure to safeguard Plaintiffs' and Class Members' Private Information, places the burden squarely on Plaintiffs and the Class, rather than on the Defendant, to investigate and protect themselves from Defendant's tortious acts and omissions resulting in the Data Breach. Defendant merely sent instructions to Plaintiffs and Class Members about actions they can affirmatively take to protect themselves.

115. Plaintiffs and Class Members have been damaged by the compromise and exfiltration, by cyber-criminals, of their Private Information as a result of the Data Breach, and by the severe disruption to their lives as a direct and foreseeable consequence of this Data Breach.

116. Plaintiffs and Class Members were damaged in that their Private Information is now in the hands of cyber criminals being sold and potentially for sale for years into the future.

117. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been placed at an actual, imminent, and substantial risk of harm from fraud

and identity theft, especially in light of the actual fraudulent misuse of the Private Information that has already taken place, as alleged herein.

118. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been forced to spend time dealing with the effects of the Data Breach.

119. Plaintiffs and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical claims billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

120. Plaintiffs and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiffs and Class Members.

121. Plaintiffs and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

122. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time monitoring their financial accounts and records for misuse.

123. Plaintiffs and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or

mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Monitoring their medical records for fraudulent charges and data;

e. Addressing their inability to withdraw funds linked to compromised accounts;

f. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

g. Placing "freezes" and "alerts" with credit reporting agencies;

h. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

i. Contacting financial institutions and closing or modifying financial accounts;

j. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

k. Paying late fees and declined payment fees imposed because of failed automatic payments that were tied to compromised cards that had to be cancelled; and

l. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

124. Moreover, Plaintiffs and Class Members have an interest in ensuring that

their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information as well as health information is not accessible online and that access to such data is password-protected.

125. Further, as a result of Defendant's conduct, Plaintiffs and Class Members are forced to live with the anxiety that their Private Information —which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

126. Defendant's delay in identifying and reporting the Data Breach caused additional harm. In a data breach, time is of the essence to reduce the imminent misuse of PII and PHI. Early notification helps a victim of a Data Breach mitigate their injuries, and in the converse, delayed notification causes more harm and increases the risk of identity theft. Here, Defendant knew of the breach ***since November 6, 2024,*** and did not notify the victims until June 26, 2025. Yet Defendant offered no explanation of purpose for the delay. This delay violates HIPAA and other notification requirements and increased the injuries to Plaintiffs and Class.

CLASS ACTION ALLEGATIONS

127. Plaintiffs bring all counts, as set forth below, individually and as a Class action, pursuant to the provisions of the Fed. R. Civ. P. 23, on behalf of a Class defined as:

> All persons whose Private Information was compromised as a result of the Data Breach that is the subject of the Notice of Data Breach published by Defendant on or about June 26, 2025 (the "Class" or "Class Members").

128. Excluded from the Class are Defendant, its subsidiaries and affiliates, officers and directors, any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

129. This proposed Class definition is based on the information available to Plaintiffs at this time. Plaintiffs may modify the Class definition in an amended pleading or when she moves for Class certification, as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

130. **Numerosity – Fed. R. Civ. P. 23(a)(1)**: Plaintiffs are informed and believe, and thereon allege, that there are at minimum, over a thousand members of the Class described above. The exact size of the Class and the identities of the individual members are identifiable through Ahold's records, including but not limited to the files implicated in the Data Breach.

131. **Commonality – Fed. R. Civ. P. 23(a)(2):** This action involves questions of law and fact common to the Class. Such common questions include, but are not limited to:

a. Whether Ahold had a duty to protect Plaintiffs' and Class members' Private Information;

b. Whether Ahold was negligent in collecting and storing Plaintiffs' and Class members' Private Information, and breached its duties thereby;

c. Whether Ahold breached its fiduciary duty to Plaintiffs and the Class;

d. Whether Ahold breached its duty of confidence to Plaintiffs and the

Class;

e. Whether Ahold violated its own Privacy Practices;

f. Whether Ahold entered a contract implied in fact with Plaintiffs and the Class;

g. Whether Ahold breached that contract by failing to adequately safeguard Plaintiffs' and Class members' Private Information;

h. Whether Ahold was unjustly enriched;

i. Whether Plaintiffs and Class members are entitled to damages as a result of Ahold's wrongful conduct; and

j. Whether Plaintiffs and Class members are entitled to restitution because of Ahold's wrongful conduct.

132. **Typicality – Fed. R. Civ. P. 23(a)(3)**: Plaintiffs' claims are typical of the claims of the members of the Class. The claims of the Plaintiffs and members of the Class are based on the same legal theories and arise from the same unlawful and willful conduct. Plaintiffs and members of the Class all had information stored in Ahold's System, each having their Private Information exposed and/or accessed by an unauthorized third party.

133. **Adequacy of Representation – Fed. R. Civ. P. 23(a)(3)**: Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the other Class members Plaintiffs seeks to represent; Plaintiffs retained counsel competent and experienced in complex Class action litigation; Plaintiffs intend to prosecute this action vigorously; and Plaintiffs' counsel has adequate financial means to vigorously pursue this action and ensure the interests of the Class will not be harmed.

Furthermore, the interests of the Class members will be fairly and adequately protected and represented by Plaintiffs and Plaintiffs' counsel.

134. **Injunctive Relief, Fed. R. Civ. P. 23(b)(2):** Defendant has acted and/or refused to act on grounds that apply generally to the Class therefore making injunctive and/or declarative relief appropriate with respect to the Class under 23(b)(2).

135. **Superiority, Fed. R. Civ. P. 23(b)(3):** A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members, which would establish incompatible standards of conduct for Ahold. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

136. Ahold has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

137. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the

disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Ahold failed to timely and adequately notify the public of the Data Breach;

b. Whether Ahold owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether Ahold's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Ahold's failure to institute adequate protective security measures amounted to negligence;

e. Whether Ahold failed to take commercially reasonable steps to safeguard consumers' and employees' Private Information; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

138. Finally, all members of the proposed Class are readily ascertainable. Ahold has access to Class members' names and addresses affected by the Data Breach. Class members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

CAUSES OF ACTION

COUNT I
Negligence
(On Behalf of Plaintiffs and Class Members)

139. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

140. Defendant required Plaintiffs and Class Members to submit non-public personal information in order to obtain healthcare services and/or employment.

141. By collecting and storing this data in Defendant's computer network and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer network—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a Data Breach.

142. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

143. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its employees, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach.

144. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the healthcare, medical, and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

145. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

146. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

147. Defendant breached its duties, and thus were negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Failure to periodically ensure that its email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and

f. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

148. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

149. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

150. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

151. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiffs and Class Members in an unsafe and unsecure manner.

152. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II

Breach of Implied Contract
(On Behalf of Plaintiffs and Class Members)

153. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

154. This Claim is pleaded in the alternative to Count III above.

155. When Plaintiffs and Class Members provided their Private Information to Defendant in exchange for Defendant's healthcare services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

156. Defendant solicited, offered, and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

157. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, including HIPAA, and were consistent with industry standards.

158. Plaintiffs and Class Members paid money to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

159. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

160. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

161. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

162. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their Private Information.

163. As a direct and proximate result of Defendant's breach of the implied contracts, Class Members sustained damages as alleged herein, including the loss of the benefit of the bargain.

164. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damage suffered as a result of the Data Breach.

165. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate long-term credit monitoring to all Class Members.

COUNT III
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and Class Members)

166. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

167. In light of the special relationship between Defendant and Plaintiffs and Class Members, whereby Defendant became guardian of Plaintiffs' and Class Members'

Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for Plaintiffs and Class Members: (1) for the safeguarding of Plaintiffs' and Class Members' Private Information; (2) to timely notify Plaintiffs and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

168. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of its relationship with its current and former employees to keep their Private Information secure.

169. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to diligently discover, investigate, and give detailed notice of the Data Breach to Plaintiffs and Class in a reasonable and practicable period of time.

170. Defendant breached its fiduciary duty to Plaintiffs and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiffs' and Class Members' Private Information.

171. Defendant breached its fiduciary duty owed to Plaintiffs and Class Members by failing to timely notify and/or warn Plaintiffs and Class Members of the Data Breach.

172. Defendant breached its fiduciary duty to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' Private Information.

173. As a direct and proximate result of Defendant's breaches of its fiduciary duty, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private

Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (vii) the diminished value of Defendant's they received.

174. As a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiffs and Class Members)

175. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

176. Plaintiffs bring this claim individually and on behalf of all Class Members.

177. This Claim is pleaded in the alternative to Count II above.

178. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiffs

and the Class Members.

179. As such, a portion of the payments made by or on behalf of Plaintiffs and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

180. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased goods from Defendant and/or its agents and in so doing provided Defendant with their Private Information. In exchange, Plaintiffs and Class Members should have received from Defendant the goods and that were the subject of the transaction and have their Private Information protected with adequate data security.

181. Defendant knew that Plaintiffs and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes.

182. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

183. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members, because

Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

184. Defendant failed to secure Plaintiffs' and Class Members' Private Information and, therefore, did not provide full compensation for the benefit Plaintiffs and Class Members provided.

185. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

186. If Plaintiffs and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have agreed to provide their Private Information to Defendant.

187. Plaintiffs and Class Members have no adequate remedy at law.

188. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the loss of the opportunity of how their Private Information is used; (c) the compromise, publication, and/or theft of their Private Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (e) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake

appropriate and adequate measures to protect Private Information in its continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

189. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

190. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Defendant's services.

COUNT V
DECLARATORY JUDGMENT
(Plaintiffs on behalf of the Class)

191. Plaintiffs restate and reallege the preceding allegations in the paragraphs above as if fully alleged herein.

192. Plaintiffs bring this claim individually and on behalf of the Class.

193. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and granting further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint.

194. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard

Plaintiffs' and Class members' PII, and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and Class members from future data breaches that compromise their PII. Plaintiffs and the Class remain at imminent risk that additional compromises of their PII will occur in the future.

195. The Court should also issue prospective injunctive relief requiring Defendant to employ adequate security practices consistent with law and industry standards to protect consumers' PII.

196. Defendant still possess Plaintiffs' and Class members' PII.

197. Defendant has made no announcement that it has changed its data storage or security practices relating to the storage of Plaintiffs' and Class members' PII.

198. To Plaintiffs' knowledge, Defendant has made no announcement or notification that it has remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

199. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at Krispy Kreme. The risk of another such breach is real, immediate, and substantial.

200. The hardship to Plaintiffs and Class members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another data breach occurs at Krispy Kreme, Plaintiffs and Class members will likely continue to be subjected to a heightened, substantial, imminent risk of fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively

minimal, and Defendant has a pre-existing legal obligation to employ such measures.

201. Issuance of the requested injunction will not compromise the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Krispy Kreme, thus eliminating the additional injuries that would result to Plaintiffs and Class members, along with other consumers whose PII would be further compromised.

202. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that Krispy Kreme implement and maintain reasonable security measures, including but not limited to the following:

a. Engaging third-party security auditors/penetration testers, as well as internal security personnel, to conduct testing that includes simulated attacks, penetration tests, and audits on Krispy Kreme's systems on a periodic basis, and ordering Krispy Kreme to promptly correct any problems or issues detected by such third-party security auditors;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training its security personnel regarding any new or modified procedures;

d. Purging, deleting, and destroying PII not necessary for its provisions of services in a reasonably secure manner;

e. Conducting regular database scans and security checks; and

f. Routinely and continually conducting internal training and education to

inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, pray for relief as follows:

a. For an Order certifying this action as a Class action and appointing Plaintiffs as a Class Representative and their counsel as Class Counsel;

b. For equitable relief enjoining Ahold from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class members;

c. For equitable relief compelling Ahold to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Personal Information compromised during the Data Breach;

d. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Ahold's wrongful conduct;

e. Ordering Ahold to pay for not less than three years of credit monitoring for Plaintiffs and the Class;

f. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g. For an award of punitive damages, as allowable by law;

h. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i. Pre- and post-judgment interest on any amounts awarded; and,

j. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury on all claims so triable.

Dated: July 8, 2025

Respectfully submitted,

By: */s/David M. Wilkerson*
David M. Wilkerson
WILKERSON JUSTUS PLLC
PO Box 54
Asheville, NC 28802
Tel: (828) 316-6902
Email: dwilkerson@wilkersonjustus.com

Liberato P. Verderame*
Marc H. Edelson*
EDELSON LECHTZIN LLP
411 S. State Street, Suite N300
Newtown, PA 18940
T: (215) 867-2399
medelson@edelson-law.com
lverderame@edelson-law.com

Attorneys for Plaintiffs and the Putative Class

* *Pro hac vice forthcoming*